



JAN 17 2006

**FACSIMILE
TRANSMISSION
FORM**

 1600 Atlanta Financial Center
 3343 Peachtree Road, N.E.
 Atlanta, Georgia 30326

Facsimile Number: 404-365-9532

This message is intended only for the use of the individual or entity to which it is addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone, and return the original message to us at the above address via U.S. Postal Service. Thank you.

TO:	U.S. Patent & Trademark Office		
NAME:	Examiner: Ronald Baum	DATE & TIME:	01/17/06
CONFIRMATION:	PAGES TO FOLLOW: 28		
FAX NUMBER:	571-273-8300		
FROM:	Morris, Manning & Martin, LLP		
NAME:	CHARGE TO:		
John R. Harris	CLIENT/MATTER: 10775-36246		
PHONE:	CONFIRMATION TIME:		
(404) 233-7000	HR	MIN	SEC

COMMENTS:
AMENDMENT AND RESPONSE TO FIRST OFFICE ACTION AND RECORD OF INTERVIEW

 Applicant: John A. Copeland III
 Docket No.: 10775-36246
 Title: FLOW-BASED DETECTION OF NETWORK INTRUSIONS

 Application No.: 10/000,396
 Filing Date: 11/30/2001

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class mail in an envelope addressed to Mail Stop Non-Fee Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, or transmitted to the U.S. Patent and Trademark Office by facsimile to number 571 273 8300 and 571-273-6741 on January 17, 2006.

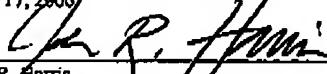
John R. Harris, Reg. No. 30,388

IF YOU HAVE ANY DIFFICULTY WITH THIS TRANSMISSION, PLEASE CALL (404) 233-7000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor: John A. Copeland III) Confirmation No.: 9056 JAN 17 2006
)
 Application No.: 10/000,396) Examiner: Ronald Baum
)
 Filed: November 30, 2001) Atty Docket: 10775-36246
) Customer No.: 24728
 Title: FLOW-BASED DETECTION OF NETWORK INTRUSIONS

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this Transmittal Letter and the papers, as described herein, are being deposited via Facsimile to 571-273-8300 addressed to: Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, on January 17, 2006.

By: 
 John R. Harris

TRANSMITTAL

Mail Stop Amendment
 Commissioner for Patents
 P.O. Box 1450
 Alexandria, VA 22313-1450

CUSTOMER NO. 24728

Sir:

We are transmitting herewith the attached:

- Transmittal Sheet containing Certificate of Facsimile Transmission (this page)
- Amendment and Response to First Office Action and Record of Interview (25 pages)
- Petition For Extension of Time (One Month) (1 page)
- Credit Card Payment Form PTO-2038 for One-Month Extension of Time in the amount of \$385.00 (1 page)

CLAIMS AS AMENDED

Claims Remaining After Amendment		Highest Number Previously Paid For		Present Extra		Rate		Fee
Total Claims								
33	-	20	=	13	x	25.00	=	\$325.00
Independent Claims								
6	-	6	=	0	x	100.00	=	\$0.00
One-Month Extension of Time								\$60.00
TOTAL FILING FEE								\$385.00

MORRIS, MANNING & MARTIN, LLP
 1600 Atlanta Financial Center
 3343 Peachtree Road NE
 Atlanta, Georgia 30326
 404-233-700 (Main)
 404-504-7720 (Direct)
 Customer No. 24728

By: 
 Name: John R. Harris
 Reg. No.: 30,388

Application No. 10/000,396
Reply to Office Action of September 15, 2005
Page 14 of 25

RECORD OF INTERVIEW

The applicants would like to thank Examiner Ronald Baum for his helpful comments and suggestions during the telephone interview with the undersigned and associate attorney Wendell Peete on December 14, 2005. During the telephone interview certain aspects of novelty over the cited art were discussed.

Pursuant to 37 C.F.R. § 1.133(b), the following description is submitted as a complete written statement of the reasons presented at the interview as warranting favorable action. The following statement is intended to comply with the requirements of MPEP § 713.04 and expressly sets forth: (A) a brief description of the nature any exhibit shown or any demonstration conducted; (B) identification of the claims discussed; (C) identification of specific prior art discussed; (D) identification of the principal proposed amendments of a substantive nature discussed; (E) the general thrust of the principal arguments; and (F) a general indication of any other pertinent matters; and (G) the general results or outcome of the interview, if appropriate.

- (A) No exhibits were shown or discussed.
- (B) The independent claims were discussed, in particular certain aspects relating to flow-based detection of network intrusions.
- (C) The *Shipley* (6,119,236) patent was discussed.
- (D) No proposed amendments were officially presented or discussed, but the claim amendments presented in this paper are consistent with the discussion.
- (E) The general thrust of the discussion was as set forth below in the next paragraphs.
- (F) No other matters were discussed.
- (G) No agreement was reached during the interview regarding the claims.

The general thrust of the discussion was that the *Shipley* patent did not disclose, teach, or suggest the claimed aspects of a flow-based detection of suspicious network activity such as intrusions. As discussed, and among other aspects, the claimed invention(s) provide for detection of suspicious network activity based on the monitoring

Application No. 10/000,396
Reply to Office Action of September 15, 2005
Page 15 of 25

of packets between two hosts on a network that are associated with a single service, and characterizing a group of such packets as a "flow."

The examiner suggested that the claims be amended to more particularly specify what a flow is and how the flows are used to determine the recited "concern index." No agreement on particular claim language was reached, pending submission of a formal amendment.

The amendments herein and comments that follow are intended to be consistent with the remarks made during the interview.

In the event that the foregoing record is not considered complete and accurate, the Examiner is respectfully requested to bring any incompleteness or inaccuracy to the attention of the undersigned.

1370936 v03